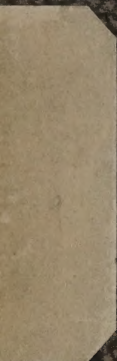
512.32
H97a



THE UNIVERSITY
OF ILLINOIS
LIBRARY
MATHEMATICS
DEPARTMENT
512.32
~~512.82~~
H97a

Arithmetische Theorie eines Galoisschen Körpers.

Inaugural-Dissertation

zur

Erlangung der Doktorwürde

der hohen

philosophischen Fakultät der Kgl. Universität Marburg

eingereicht

und mit ihrer Genehmigung veröffentlicht

von

Friedrich Hüttig

aus Sagan in Schlesien.

Marburg

1907.

LIBRARY
UNIVERSITY OF ILLINOIS
URBANA

Von der Fakultät als Dissertation angenommen

am 21. Februar 1906.

Referent: Professor Dr. **K. Hensel.**

512.82
H97a

Meinem verehrten Lehrer

Herrn Professor Dr. Hensel.

Mathematics Research 22Ap'14 Stechert 35

264793

In folgender Arbeit will ich die Behandlungsweise der algebraischen Zahlen, die neuerdings von Herrn Prof. Hensel eingeführt wurde, auf einen Galoisschen Zahlenkörper anwenden.

Zu ihrem Verständnis sollen die Hauptpunkte jener Theorie, die ich aus drei Abhandlungen[1]) sowie durch mündliche Mitteilungen kennen lernte, vorausgeschickt werden.

A. Allgemeiner Teil:

Untersuchung einer algebraischen Zahl für den Bereich einer Primzahl p.

I. Die rationalen Zahlen und der Bereich K(1). Der erweiterte Bereich K(p). Ganze rationale Funktionen in dem Bereiche K(p).

§ 1. Die ganzen rationalen Zahlen A lassen sich in eindeutiger Weise nach steigenden Potenzen einer Primzahl p in der Form

$$A = a_0 + a_1 p + \cdots + a_m p^m$$

entwickeln, wo die Koeffizienten $a_0, \cdot\cdot\, a_m$ Zahlen der Reihe $0, 1 \cdots (p-1)$ sind.

---

[1]) Journal für reine und angewandte Mathematik, Bd. 127, H. 1: Neue Grundlagen der Arithmetik. Bd. 128, H. 1: Ueber eine neue Begründung der Theorie der algebraischen Zahlen. — Mathematische Annalen. Bd. 55: Ueber die Entwickelung der algebraischen Zahlen in Potenzreihen.

So besteht z. B. die Entwicklung

$$123 = 4 + 3 \cdot 7 + 2 \cdot 7^2$$

oder in vereinfachter Form geschrieben:

$$123 = 4{,}32. \qquad (7)$$

§ 2. Um die Subtraktion und Division der ganzen Zahlen allgemein zu ermöglichen, wird der Zahlbegriff in folgender Weise erweitert.

Man definiert die Differenz $X = A - B$, bez. den Quotienten $Y = \frac{A}{B}$ durch folgende Kongruenzen:

$$X + B \equiv A \quad (\mathrm{mod}\ p^k)$$
$$YB \equiv A \quad (\mathrm{mod}\ p^k),$$

wo k beliebig gross genommen werden kann.

Aus diesen Kongruenzen können X und Y als im allgemeinen nicht abbrechende nach ganzen Potenzen von p fortschreitende Reihen beliebig weit in eindeutiger Weise berechnet werden. Diese Reihen sind inbezug auf die Reihenfolge der Koeffizienten rein oder gemischt periodisch. Der Quotient Y kann auch negative Potenzen von p enthalten.

Die Gesamtheit aller rationaler Zahlen, welche sich alle in solche periodischen Reihen entwickeln lassen, soll der Bereich K(1) genannt werden.

Als Beispiele für X und Y seien folgende Zahlen angeführt:

$$5{,}23666 \cdots = 1{,}531 - 3{,}202$$
$$2{,}26402\,6402 \cdots = \frac{5{,}3}{6{,}2} \qquad (7)$$

§ 3. Eine Zahl A aus K(1) ist gleich der Zahl B für den Bereich von p, als Gleichung geschrieben

$$A = B \qquad (p),$$

wenn die Kongruenz

$$A \equiv B \quad (\mathrm{mod}\ p^k)$$

für beliebig grosses k besteht. Eine Zahl ist also für den Bereich von p gleich Null, wenn sie durch jede noch so hohe Potenz von p teilbar ist.

§ 4. Der Bereich K(1) wird erweitert zu dem Bereiche K(p), in welchen alle nach ganzen Potenzen von p fortschreitende Reihen aufgenommen werden, welche sich nach irgend einem Gesetze beliebig weit berechnen lassen.

Ganze rationale Funktionen, die in K(1) irreduzibel waren, können in dem erweiterten Bereiche K(p) reduzibel werden. So besteht für die in K(1) irreduzible Funktion

$$f(x) = x^2 - 2$$

im Bereiche K(7) die Zerlegung in zwei lineare Faktoren

$$f(x) = (x - 3{,}1261 \cdots)(x - 4{,}5405 \cdots) \qquad (7),$$

d. h. es besteht für beliebig grosses k die Kongruenz

$$x^2 - 2 \equiv (x - 3{,}1261 \cdots)(x - 4{,}5405 \cdots) \quad \mathrm{mod}\ 7^{(k)}$$

Dagegen bleibt die Funktion

$$\varphi(x) = x^2 - 5$$

auch innerhalb des erweiterten Bereiches K(7) irreduzibel, da die Zahl 5 quadratischer Nichtrest von 7 ist.

§ 5. Eine durch p nicht teilbare Zahl heisst eine „Einheit für den Bereich von p“. Jede Zahl A aus K(p) ist offenbar gleich einer ganzen Potenz von p mal einer Einheit E für den Bereich von p

$$A = p^{\rho} \cdot E.$$

ρ heisst die Ordnung der Zahl A inbezug auf p. Die Ordnung eines Produktes bez. eines Quotienten aus zwei Zahlen ist gleich der Summe bez. Differenz der Ordnungen dieser Zahlen.

§ 6. Für den Bereich K(p) besteht folgender wichtige Satz, auf welchem die Bedeutung seiner Einführung beruht:

Jede im Bereiche K(p) rationale ganze Funktion lässt sich durch ein endliches Verfahren in eindeutiger Weise in Faktoren zerlegen, deren Koeffizienten dem

Bereiche K(p) angehören, und welche in K(p) irreduzibel sind. (Neue Grundlagen, S. 77).

Dieser Satz ist das zahlentheoretische Analogon zu dem Gaussschen Fundamentalsatze der Algebra, welcher besagt, dass sich jede rationale ganze Funktion in lineare oder quadratische Faktoren zerlegen lässt, deren Koeffizienten nach ganzen fallenden Potenzen einer von 1 verschiedenen ganzen Zahl fortschreiten.

II. Die Teilbarkeit der algebraischen Zahlen in bezug auf die Primzahl p. Reihenentwicklungen.

§ 7. Eine algebraische Zahl α heisst ganz für den Bereich von p, wenn in einer der sie definierenden Gleichungen

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0$$

sämtliche Koeffizienten von nicht negativer Ordnung in bezug auf p sind. Die algebraische Zahl α heisst teilbar durch die Zahl β, wenn $\frac{\alpha}{\beta}$ eine ganze algebraische Zahl ist.

Eine ganze algebraische Zahl ist eine Einheit in bezug auf p, wenn der letzte Koeffizient a_n, d. i. die Norm, eine Einheit in bezug auf p ist.

Wenn die ganze Zahl α durch eine ganze oder gebrochene Potenz von p teilbar sein soll, so müssen, wie leicht zu sehen, sämtliche Koeffizienten $a_1, a_2, \cdots a_n$ mindestens durch p teilbar sein. Somit kann es algebraische Körper geben, in welchen Zahlen durch keine ganze oder gebrochene Potenz von p teilbar und trotzdem keine Einheiten sind, wie man sich an Beispielen überzeugen kann.

§ 8. Dieser Umstand bewirkt, dass die Teilbarkeitsgesetze der algebraischen Zahlen nicht so einfach sind wie die der rationalen Zahlen. Für eine algebraische Zahl jedoch, deren Gleichung in K(p) irreduzibel ist (vergl. § 6), kommt diese Schwierigkeit nicht in betracht. Denn für sie besteht der wichtige Satz: (Neue Grundlagen, S. 13)

Eine für den Bereich von p ganze algebraische Zahl, deren Gleichung in K(p) irreduktibel ist, ist ent-

weder eine Einheit oder durch eine ganze oder gebrochene Potenz von p teilbar.

Man kann daher alle Grössen α eines durch eine solche algebraische Zahl bestimmten Körpers in der Form

$$\alpha = p^{\rho} \cdot e$$

darstellen, iu welcher e eine algebraische Einheit für den Bereich von p und ρ eine ganze oder gebrochene rationale Zahl ist. Wenn ρ gebrochen ist, wird e im allgemeinen nicht dem betreffenden Körper angehören.

Ist

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

die in K(p) irreduzible Gleichung der algebraischen Zahl α, so ist die Norm a_n, wie leicht zu sehen, genau durch $p^{\rho n}$ teilbar.

§ 9. Um aber die algebraischen Zahlen so darstellen zu können, wie früher die rationalen, sucht man eine ganze Grösse π aus dem Körper $K(\alpha)$, welche durch die niedrigste Potenz von p teilbar ist. Man braucht zu diesem Zwecke nur aus einer endlichen Anzahl von ganzen Grössen des Körpers eine solche auszusuchen, deren Norm durch die niedrigste Potenz von p teilbar ist. (Neue Begründung, S. 15)

Es folgt dann leicht, dass die Zahl π durch eine Potenz von der Form $p^{\frac{1}{e}}$ genau teilbar ist, wo e ein Teiler von n ist.

Jede Grösse des Körpers $K(\alpha)$ lässt sich nun in der Form

$$\pi^{\rho} \varepsilon$$

darstellen, wo ε nunmehr eine Einheit aus $K(\alpha)$ und ρ eine ganze rationale Zahl ist. Der Exponent ρ heisst die Ordnungszahl in bezug auf die Primzahl p. Es gelten die Sätze:

Eine Zahl aus $K(\alpha)$ ist dann und nur dann für den Bereich von p algebraisch ganz, wenn ihre Ordnungszahl nicht negativ ist.

Die Ordnungszahl eines Produktes, bez. Quotienten zweier Zahlen ist gleich der Summe, bez. Differenz der Ordnungszahlen.

Zwei Zahlen heissen äquivalent für den Bereich von p, wenn sie dieselbe Ordnungszahl besitzen. Zwei Zahlen sind modulo π kongruent, wenn ihre Differenz durch π teilbar ist.

§ 10. Man kann aus einem vollständigen System von modulo p inkongruenten Grössen des Körpers, deren Anzahl bekanntlich gleich p^n ist, ein vollständiges System von modulo π inkongruenten Grössen aussuchen. Dann ist jede Grösse des Körpers $K(\alpha)$ einer von diesen Grössen modulo π kongruent, und daraus folgt, dass man jede Grösse γ des Körpers in eine nach steigenden Potenzen von π fortschreitende Reihe in eindeutiger Weise entwickeln kann:

$$\gamma = \varepsilon_\rho \pi^\rho + \varepsilon_{\rho+1} \pi^{\rho+1} + \cdots,$$

wo die Koeffizienten ε_ρ, $\varepsilon_{\rho+1}, \ldots$ Einheiten aus jenem vollständigen System sind.

Man kann auf einfache Weise zeigen, dass ein solches vollständiges System aus p^f Grössen besteht, wo $e \cdot f = n$ ist. Die Zahl f hat die besondere Eigenschaft, dass jede Grösse des Körpers der Kongruenz

$$x^{p^f} - x \equiv 0 \qquad (\text{mod } \pi)$$

genügt.

III. Der aus K(p) und K(α) zusammengesetzte erweiterte Bereich K(p,α).

§ 11. Es soll nunmehr der grössere Bereich $K(p,\alpha)$ betrachtet werden, der alle rationalen Funktionen von α mit Koeffizienten aus $K(p)$ umfasst. Die Grössen dieses erweiterten Bereiches sind Wurzeln von Gleichungen n^{ten} Grades, deren Koeffizienten dem Körper $K(p)$ angehören.

In dem erweiterten Bereiche $K(p,\alpha)$ kann man ein vollständiges System von modulo π inkongruenten Grössen auswählen, welches sehr einfache Eigenschaften besitzt. Dieses System wird durch den Ausdruck

$$e_0 + e_1 \varepsilon + \cdots + e_{f-1} \varepsilon^{f-1} \qquad [e_i = 0, 1, \cdots (p-1)] \qquad (1)$$

dargestellt, wo ε primitive Wurzel der Gleichung

$$x^{p^f-1} - 1 = 0$$

ist. Die linke Seite dieser Gleichung ist in K(p) reduzibel. Und zwar ist ε Wurzel eines in K(p) irreduktiblen Faktors f^{ten} Grades

$$\varphi(x) = x^f + c_1 x^{f-1} + \cdot\cdot + c_f .$$

Diese Gleichung ist auch modulo p betrachtet irreduktibel.

Man kann leicht zeigen, dass ε^p, ε^{p^2}, $\cdot\cdot$ $\varepsilon^{p^{f-1}}$ die übrigen Wurzeln von $\varphi(x)$ sind, so dass also die Identität

$$\varphi(x) = (x-\varepsilon)(x-\varepsilon^p) \cdots (x-\varepsilon^{p^{f-1}})$$

besteht.

Die Grössen des vollständigen Systems (1) gehören also zu einem Körper, der im Rationalitätsbereiche K(p) vom f^{ten} Grade ist. Dieser Unterkörper von $K(p,\alpha)$ wird der Koeffizientenkörper $K(\varepsilon)$ genannt.

Die Grösse π kann nunmehr durch eine äquivalente Grösse aus $K(p,\alpha)$ ersetzt werden, die einer Gleichung von der Form

$$\psi(x) = x^e + c_{e-1}\, p x^{e-1} + \cdot\cdot + c_0 p = 0$$

genügt, wo die Koeffizienten c_i ganze Zahlen des Körpers $K(1,\varepsilon)$ sind und c_0 eine Einheit dieses Körpers ist.

In dem Falle, dass e durch p nicht teilbar ist, hat die Gleichung $\psi(x) = 0$ die einfache Form

$$x^e + c_0 p = 0,$$

wo c_0 eine Einheit aus $K(1,\varepsilon)$ ist. (Neue Begründung, S. 32)

Die Grössen von $K(p,\alpha)$ lassen sich nun ebenso wie in § 10 auch mit Hilfe der neuen Entwicklungsgrössen ε und π eindeutig in Reihen entwickeln

$$\gamma = \varepsilon^{(\rho)}\pi^{(\rho)} + \varepsilon^{(\rho+1)}\pi^{\rho+1} + \cdots ,$$

in welchen die Koeffizienten $\varepsilon^{(\rho)}$, $\varepsilon^{(\rho+1)}$ $\cdots$ dem Systeme (1) angehören. Die $n = e \cdot f$ Konjugierten von γ gehen aus einer von ihnen dadurch hervor, dass man ε sämtliche f Wurzeln ε, ε^p, ε^{p^2} $\cdots$ der Gleichung

$$\varphi(x) = 0$$

und π jedesmal die e Wurzeln der zugehörigen Gleichung

$$\psi(x) = 0$$

durchlaufen lässt.

Man sieht daraus, dass die $n = e \cdot f$ konjugierten Werte γ durch dieselbe Potenz $p^{\frac{\rho}{e}}$ von p genau teilbar sind, sowie dass ihre Norm genau durch $p^{\rho \cdot f}$ teilbar ist.

IV. Teilbarkeit der algebraischen Zahlen in bezug auf die Primzahl p im allgemeinen Falle.

§ 12. Die Funktion f(x) möge nunmehr in K(p) zerlegbar sein und in mehrere Faktoren zerfallen,

$$f(x) = f_1(x) \cdot f_2(x) \cdot \cdot \cdot \cdot f_\nu(x)$$

dann lassen sich die Wurzeln jedes der Faktoren in der in § 11 beschriebenen Weise entwickeln.

Die Gesamtheit der Wurzeln von f(x) besteht jetzt aus ν zu den Faktoren $f_1(x), \cdot \cdot \cdot f_\nu(x)$ gehörigen Cyklen. Die Wurzeln jedes dieser Cyklen verhalten sich in bezug auf ihre Teilbarkeit durch die Primzahl p gleich.

Im allgemeinen werden die Entwicklungsgrössen ε und π in jedem der Cyklen von einander verschiedene algebraische Zahlen sein.

§ 13. Auf Grund des § 9 kann man folgende Teilbarkeitsgesetze aufstellen:

Eine algebraische Zahl des Körpers $K(\alpha)$ ist für den Bereich von p ganz, wenn die Wurzeln jedes der ν Cyklen von positiver Ordnung sind. Eine algebraische Zahl ist also durch eine andere dann und nur dann teilbar, wenn sie mindestens von derselben Ordnung wie diese in jedem der Cyklen ist.

Wenn man sich der in der Dedekindschen Idealtheorie gebräuchlichen Ausdrucksweise bedienen will, so ordnet man den irreduziblen Faktoren $f_1(x), f_2(x), \cdot \cdot f_\nu(x)$ der Reihe nach die idealen Primfaktoren $\mathfrak{p}_1, \mathfrak{p}_2, \cdot \cdot \mathfrak{p}_\nu$ zu und sagt,

dass p innerhalb des vorliegenden Körpers in ν ideale Primfaktoren zerfällt. Eine Zahl des Körpers „enthält den idealen Primfaktor p_i in der ρ^{ten} Potenz", wenn ihre zum Wurzelcyklus von $f_i(x)$ gehörigen Entwicklungen mit der ρ^{ten} Potenz von π beginnen. Wenn die Zahlen e und f für den Faktor $f_i(x)$ die oben gebrauchte Bedeutung haben, so sagt man, der Primfaktor p_i hat den Grad f und die Ordnung e.

§ 14. Bezeichnet f wie bisher den Grad des Koeffizientenkörpers, ist $\psi'(\pi)$ die Ableitung von $\psi(\pi)$ nach π und $e'-1$ die Ordnung der Zahl $\psi'(\pi)$ in bezug auf p, so ist die Diskriminante des Körpers genau durch

$$\Pi p^{f(e'-1)}$$

teilbar, wo das Produkt über sämtliche in K(p) irreduktible Faktoren der den Körper definierenden Gleichung erstreckt wird. (Mathem. Annalen. Bd. 55).

V. Einige Bemerkungen über die als Wurzeln von Gleichungen betrachteten Reihenentwicklungen.

§ 15. Es sei f(x) eine in K(p) irreduzible Funktion mit Koeffizienten aus K(1) oder K(p) vom n^{ten} Grade. $\bar{\alpha}$ sei eine Wurzel von $f(x) = 0$. Dann kann man in dem erweiterten Bereiche $K(p,\bar{\alpha})$, wie oben auseinandergesetzt wurde, die Grössen ε und π berechnen. ε genügt der in K(p) irreduziblen Gleichung f^{ten} Grades

$$\varphi(x) = 0$$

mit ganzen Koeffizienten aus K(p). π genügt der in $K(p,\varepsilon)$ irreduziblen Gleichung e^{ten} Grades

$$\psi(x) = 0$$

mit ganzen Koeffizienten aus $K(1,\varepsilon)$. Der Körper $K(\pi,\varepsilon)$ ist identisch mit $K(p,\bar{\alpha})$. Was man unter $\bar{\alpha}$ zu verstehen hat, ist gleichgültig. Jedenfalls kann man aus den Koeffizienten von f(x) diejenigen von $\varphi(x)$ und $\psi(x)$ berechnen.

Ich will hier hervorheben, dass man sich unter ε und π nicht irgend welche Zahlenwerte vorzustellen hat. Es sind Symbole, die durch ihre Gleichungen definiert sind und die den für die algebraischen Grössen geltenden Rechenregeln unterworfen sind. Ihre Einführung ist ähnlich der Einführung der imaginären Grösse i, die ja auch durch eine unlösbare Gleichung, $x^2 + 1 = 0$, definiert ist.

Im folgenden soll die Grösse π stets primitiv in bezug auf K(p) angenommen werden. Sollte das noch nicht der Fall sein, so kann man ihr diese Eigenschaft durch Multiplikation mit einer geeigneten Einheit aus $K(\varepsilon)$ stets verschaffen. Man kann dann den Körper $K(\pi,\varepsilon)$ auch kurz mit $K(\pi)$ bezeichnen. π genügt dann einer in K(p) irreduziblen Gleichung n^{ten} Grades

$$\Psi(x) = x^n + p^f c_{n-1} x^{n-1} + \cdots + p^f c_0 = 0,$$

deren Koeffizienten ganze Zahlen des Bereiches K(p) sind. Und zwar ist c_0 eine Einheit.

§ 16. Jede Grösse ρ des Körpers $K(p,\bar{\alpha})$ lässt sich dann als eine in K(p) rationale Funktion von π darstellen. Diese Darstellungsmöglichkeit wird im folgenden nur gelegentlich gebraucht werden.

Es wird dagegen hier stets von der oben erörterten Reihendarstellung

$$\rho = e_\lambda \pi^\lambda + e_{\lambda+1} \pi^{\lambda+1} + \cdots$$

ausgegangen werden.

Wir definieren entsprechend dem § 3: Eine algebraische Grösse ρ des Körpers $K(\pi,\varepsilon)$ ist gleich Null,

$$\rho = 0,$$

wenn ρ, genügend weit berechnet, der Kongruenz

$$\rho \equiv 0 \pmod{\pi^{\mathfrak{L}}}$$

für beliebig grosses $\mathfrak{L}$ genügt.

Entwickeln wir eine Wurzel der Gleichung $f(x) = 0$ nach π und nennen die entstehende Reihe α, so ist nach dieser Definition

$$f(\mathfrak{x}) = 0.$$

Wir nennen α eine „Wurzel“ von $f(x) = 0$. Im folgenden soll das Wort „Wurzel“ stets in diesem Sinne verstanden werden, wenn nicht ausdrücklich etwas anderes darüber bestimmt wird.

§ 17. Man kann ebenso wie in der Algebra auf Grund des Euklidschen Verfahrens folgende Sätze beweisen:

1. Ist $f(x)$ irreduzibel in $K(p)$ und verschwindet $F(x)$ für eine Wurzel der Gleichung $f(x) = 0$, so ist die Funktion $F(x)$ durch $f(x)$ teilbar.

2. Unter denselben Voraussetzungen verschwindet also $F(x)$ auch für sämtliche übrigen Wurzeln von $f(x)$.

3. Ist aber $F(x)$ von niedrigerem Grade als $f(x)$, so müssen die Koeffizienten von $F(x)$ gleich Null sein.

Die drei Sätze bleiben bestehen, wenn man statt des Körpers $K(p)$ den durch eine beliebige Irrationalitat ξ aus $K(\pi, \varepsilon)$ erweiterten Körper $K(p, \xi)$ nimmt, $F(x)$ und $f(x)$ Funktionen in diesem Körper sind und $f(x)$ irreduzibel ist in diesem Körper.

B. Anwendung der allgemeinen Theorie auf einen Galoisschen Körper.

§ 1. Die Galoissche Gleichung und ihre Gruppe.

Die Resultate der allgemeinen Theorie sollen nun auf einen Galoisschen Körper angewandt werden, d. h. auf einen Körper, der mit seinen konjugierten identisch ist.

Er sei definiert durch die Wurzeln der Galoisschen Gleichung

$$F(x) = 0$$

vom Grade N; und zwar sollen diese Wurzeln ganze Zahlen sein. Wir wollen sie zunächst wie in der Algebra in bezug auf die Grösse betrachten, nicht als nach Potenzen von π fortschreitende Reihen.

Die irreduzible Funktion F(x) hat die Eigenschaft, dass sich jede ihre Wurzeln durch jede andere rational ausdrücken lässt. Die Wurzeln seien folgende:

$$\bar{\alpha},\ \Theta_1(\bar{\alpha}),\ \Theta_2(\bar{\alpha}),\ \cdots\ \Theta_{N-1}(\bar{\alpha}).$$

Es ist also allgemein

$$F[\Theta_i(\bar{\alpha})] = 0.$$

Diese Gleichung kann bekanntlich nur dann bestehen, wenn die Funktion $F[\Theta_i(x)]$ durch F(x) teilbar ist, wenn also z. B. die Identität besteht:

$$F[\Theta_i(x)] = g(x) \cdot F(x), \qquad (1)$$

wo g(x) eine ganze Funktion ist.

Wir gehen nunmehr zu den nach Potenzen von π fortschreitenden Wurzeln der Gleichung $F(x) = 0$ über. α sei eine solche Wurzel, es sei also

$$F(\alpha) = 0$$

in dem in § 16 definierten Sinne, d. h. $F(\alpha)$ sei durch jede noch so hohe Potenz von π teilbar. Dann folgt aus der Gleichung (1) die andere:

$$F[\Theta_i(\alpha)] = 0.$$

Es ist folglich auch $\Theta_i(\alpha)$ Wurzel von $F(x) = 0$. Wir haben also für F(x) folgende Wurzeln

$$\alpha,\ \Theta_1(\alpha),\ \Theta_2(\alpha),\ \cdots\ \Theta_{N-1}(\alpha). \qquad (2)$$

F(x) hat auch nicht mehr Wurzeln. Denn die Grössen (2) sind alle von einander verschieden, da die Diskriminante von F(x) von Null verschieden ist.

Die von den Wurzeln gebildete Gruppe möge mit G bezeichnet werden.

§ 2. Die Zerlegung der Galoisschen Gleichung in ihre für den Bereich von p irreduktiblen Faktoren.

Es möge f(x) innerhalb K(p) in ν irreduktible Faktoren zerfallen:

$$F(x) = f_1(x) \cdot f_2(x) \cdots f_\nu(x),$$

so dass innerhalb des Galoisschen Körpers ν von einander verschiedene in p aufgehende ideale Primfaktoren existieren, welche der Reihe nach mit

$$\mathfrak{p}_1, \mathfrak{p}_2, \cdots \mathfrak{p}_\nu$$

bezeichnet werden sollen.

$f_1(x)$ habe den Grad n und die Wurzeln

$$\alpha, \Theta_1(\alpha), \Theta_2(\alpha), \cdots \Theta_{n-1}(\alpha). \qquad (1)$$

Diese gehören zu einer Untergruppe der Galoisschen Gruppe G, welche mit Z bezeichnet und Zerlegungsgruppe genannt werden soll.

Denn sei $\Theta_i(\alpha)$ eine der Wurzeln (1), so muss $f_1[\Theta_i(x)]$ als Funktion von x aufgefasst nach § 17 durch die irreduzible Funktion $f_1(x)$ teilbar sein, da sie mit dieser die Wurzel $x = \alpha$ gemeinsam hat. Sie muss also auch für $x = \Theta_k(\alpha)$ verschwinden, wo $\Theta_k(\alpha)$ eine beliebige der Wurzeln (1) bedeutet:

$$f_1[\Theta_i \Theta_k(\alpha)] = 0.$$

Die Grösse $\Theta_i \Theta_k(\alpha)$ ist also wieder Wurzel von $f_1(x)$, ist demnach eine der Wurzeln (1), wodurch die Gruppeneigenschaft dieser Wurzeln nachgewiesen ist.

Es sei ferner $g_i(\alpha)$ eine nicht zu (1) gehörige Wurzel von F(x). Sie muss dann Wurzel eines der übrigen irreduzibeln Faktoren von F(x), z. B. des Faktors $f_i(x)$ sein. $f_i[g_i(x)]$ hat als Funktion von x aufgefasst die Wurzel $x = \alpha$ mit $f_1(x)$ gemeinsam, ist also teilbar durch $f_1(x)$ und hat somit sämtliche Grössen (1) zu Wurzeln. Oder, was dasselbe sagt, $f_i(x)$ besitzt die n verschiedenen Wurzeln

$$g_i(\alpha), g_i[\Theta_1(\alpha)], \cdots g_i[\Theta_{n-1}(\alpha)].$$

$f_i(x)$ hat auch nicht mehr Wurzeln. Denn da sich α auch rational durch $g_i(\alpha)$ ausdrücken lässt, so beweist man ebenso umgekehrt, dass $f_1(x)$ mindestens ebensoviele Wurzeln wie $f_i(x)$ haben muss.

Sämtliche irreduktible Faktoren von F(x) haben demnach denselben Grad n. Ist ihre Anzahl gleich ν, so besteht die Beziehung:

$$N = \nu \cdot n.$$

Die Anzahl ν der in der Primzahl p aufgehenden von einander verschiedenen Primfaktoren muss also ein Teiler des Grades N der Galoisschen Gleichung sein.

Die Wurzeln der einzelnen irreduziblen Faktoren von F(x)

$$f_1(x),\ f_2(x), \cdots f_\nu(x)$$

gehen nun der Reihe nach durch die Substitutionen der Nebengruppen

$$Z,\ g_1 Z, \cdots g_{\nu-1} Z \qquad (2)$$

aus α hervor. Sie sollen in abkürzender Weise mit

$$Z(\alpha),\ g_1 Z(\alpha), \cdots g_{\nu-1} Z(\alpha)$$

bezeichnet werden.

Für die Nebengruppen (2) gelten folgende gruppentheoretischen Sätze: (cfr. Weber, Algebra, 2. Aufl., Bd. I § 161, Satz 2).

Wenn h eine beliebige Substitution der Gruppe G ist, so stimmt die Reihe

$$hZ,\ hg_1 Z, \cdots hg_{\nu-1} Z$$

abgesehen von der Anordnung mit der Reihe der Nebengruppen (2) überein. Bei einer solchen Substitution geht die Gruppe Z in sich selbst über, wenn h der Gruppe Z selbst angehört. Die Nebengruppe $g_i Z$ geht in sich selbst über, wenn h der zu Z konjugierten Gruppe $g_i Z g_i^{-1}$ angehört.

Betrachtet man eine beliebige primitive Grösse $\rho(\alpha)$ des Galoisschen Körpers, d. h. eine solche, die einer im gewöhnlichen Rationalitätsbereiche irreduziblen Gleichung, z. B. R(x), vom N^{ten} Grade genügt, so zerfällt diese Gleichung im Bereiche K(p) offenbar wieder in ν irreduzible Faktoren vom Grade n:

$$R(x) = r_1(x) \cdot r_2(x) \cdots r_r(x).$$

Die Wurzeln der auf der rechten Seite stehenden Faktoren lassen sich nun in ähnlicher Weise wie oben in der Form

$$\rho[Z(\alpha)],\ \rho[g_1 Z(\alpha)],\ \cdots\ \rho[g_{\nu-1} Z(\alpha)]$$

zusammenfassen.

Wendet man auf $\rho(\alpha)$ die beliebige in G enthaltene Substitution h an, so geht $\rho(\alpha)$ in $\rho[h(\alpha)]$ über. $\rho[h(\alpha)]$ genügt offenbar wieder derselben Gleichung R(x); aber die in K(p) irreduziblen Faktoren folgen jetzt in andrer Reihenfolge aufeinander. Sie enthalten nämlich der Reihe nach die Wurzelkomplexe:

$$\rho[hZ(\alpha)],\ \rho[hg_1 Z(\alpha)],\ \cdots\ \rho[hg_{\nu-1} Z(\alpha)],$$

welche uns in dieser Reihenfolge über die Teilbarkeit von $\rho[h(\alpha)]$ durch die Primfaktoren

$$p_1,\ p_2,\ \cdots\ p_\nu$$

Aufschluss geben.

Wenn nun $\rho(\alpha)$ durch die Primfaktorpotenz $p_i{}^b$ teilbar war, so ist es $\rho[h(\alpha)]$ durch $p_k{}^b$, wenn durch die vorn ausgeführte Substitution h die Wurzeln von $r_k(x)$ übergeführt werden in die Wurzeln von $r_i(x)$. Dagegen ist wiederum $\rho[h(\alpha)]$ durch $p_i{}^b$ teilbar, wenn h der Gruppe $g_i Z g_i{}^{-1}$ angehört. War $\rho(\alpha)$ durch $p_1{}^b$ teilbar, so ist es auch $\rho[h(\alpha)]$, wenn h der Gruppe Z angehört.

Wenden wir die Resultate auf die Gesamtheit aller Zahlen des Körpers an, welche durch einen der Primfaktoren p_i teilbar sind, d. h. auf ein Primideal an, so besagt das Vorhergehende in der Sprache der Dedekindschen Idealtheorie:

Jedes Primideal des Galoisschen Körpers geht durch eine Substitution der Galoisschen Gruppe wieder in ein Primideal über, welches dem ersteren konjugiert ist.

Das Primideal p_1 bleibt durch die Substitutionen der Gruppe Z ungeändert. Das zu p_1 konjugierte Primideal p_i bleibt durch die Substitutionen der Gruppe $g_i Z g_i{}^{-1}$ ungeändert.

§ 3. Die Entwickelungsgrössen ε und π der irreduktiblen Faktoren von F(x).

Da unser Körper mit seinen konjugierten identisch ist, so können für alle Faktoren von F(x) dieselben Entwickelungsgrössen ε und π genommen werden. Es folgt daraus, dass die Primzahl p innerhalb eines Galoisschen Körpers in ideale Primfaktoren von gleicher Ordnung und gleichem Grade zerfällt, die denselben Zerlegungsgesetzen gehorchen. Aus diesem Grunde genügt es, zur Untersuchung dieser Gesetze nur einen der ν Faktoren von F(x) zu betrachten. Wir wollen ihn mit f(x) bezeichnen und ihm, um uns auch der Dedekindschen Ausdrucksweise bedienen zu können, den idealen Primfaktor $\mathfrak{p}$ zuordnen.

§ 4. Die Wurzeln eines in K(p) irreduktiblen Faktors f(x) der Galoisschen Gleichung F(x).

Nach der allgemeinen Theorie lassen sich die Wurzeln von f(x) folgendermassen anordnen:

$$\begin{array}{l}
\alpha = \alpha_{11} = \Theta_{11}(\alpha) = \varepsilon_1^{(\rho)}\,\pi_{11}^{\rho} + \varepsilon_1^{(\rho+1)}\,\pi_{11}^{\rho+1} + \cdots \\
\phantom{\alpha = {}}\alpha_{12} = \Theta_{12}(\alpha) = \varepsilon_1^{(\rho)}\,\pi_{12}^{\rho} + \varepsilon_1^{(\rho+1)}\,\pi_{12}^{\rho+1} + \cdots \\
\qquad \cdot \quad \cdot \quad \cdot \quad \cdot \\
\qquad \cdot \quad \cdot \quad \cdot \quad \cdot \\
\phantom{\alpha = {}}\alpha_{1e} = \Theta_{1e}(\alpha) = \varepsilon_1^{(\rho)}\,\pi_{1e}^{\rho} + \varepsilon_1^{(\rho+1)}\,\pi_{1e}^{\rho+1} + \cdots \\
\hline
\phantom{\alpha = {}}\alpha_{21} = \Theta_{21}(\alpha) = \varepsilon_2^{(\rho)}\,\pi_{21}^{\rho} + \varepsilon_2^{(\rho+1)}\,\pi_{21}^{\rho+1} + \cdots \\
\phantom{\alpha = {}}\alpha_{22} = \Theta_{22}(\alpha) = \varepsilon_2^{(\rho)}\,\pi_{22}^{\rho} + \varepsilon_2^{(\rho+1)}\,\pi_{22}^{\rho+1} + \cdots \\
\qquad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\
\qquad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\
\phantom{\alpha = {}}\alpha_{2e} = \Theta_{2e}(\alpha) = \varepsilon_2^{(\rho)}\,\pi_{2e}^{\rho} + \varepsilon_2^{(\rho+1)}\,\pi_{2e}^{\rho+1} + \cdots \\
\hline
\qquad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\
\qquad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\
\qquad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\
\hline
\phantom{\alpha = {}}\alpha_{f1} = \Theta_{f1}(\alpha) = \varepsilon_f^{(\rho)}\,\pi_{f1}^{\rho} + \varepsilon_f^{(\rho+1)}\,\pi_{f1}^{\rho+1} + \cdots \\
\phantom{\alpha = {}}\alpha_{f2} = \Theta_{f2}(\alpha) = \varepsilon_f^{(\rho)}\,\pi_{f2}^{\rho} + \varepsilon_f^{(\rho+1)}\,\pi_{f2}^{\rho+1} + \cdots \\
\qquad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot\;\cdot \\
\qquad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot\;\cdot \\
\phantom{\alpha = {}}\alpha_{fe} = \Theta_{fe}(\alpha) = \varepsilon_f^{(\rho)}\,\pi_{fe}^{\rho} + \varepsilon_f^{(\rho+1)}\,\pi_{fe}^{\rho+1} + \cdots
\end{array}$$

Die Koeffizienten $\varepsilon_1^{(k)}$ in diesem Schema sind reduzierte Grössen des Koeffizientenkörpers $K(\varepsilon)$, d. h. Grössen von der Form

$$c_0 + c_1 \varepsilon + \cdots + c_{f-1} \varepsilon^{f-1} \qquad [c_i = 0, 1, \cdots (p-1)],$$

wo ε eine primitive Wurzel der Gleichung

$$x^{p^f - 1} - 1 = 0$$

ist; und zwar ist ε Wurzel eines in $K(p)$ irreduktiblen Faktors f^{ten} Grades von $(x^{p^f-1} - 1)$. ε^p, ε^{p^2}, $\cdots$ $\varepsilon^{p^{f-1}}$ sind die übrigen Wurzeln dieses Faktors.

Es entsteht allgemein

$$\varepsilon_i^{(k)} \quad \text{aus} \quad \varepsilon_1^{(k)}$$

dadurch, dass man in $\varepsilon_1^{(k)}$ die Grösse ε durch die konjugierte ε^{p^i} ersetzt.

Die Entwickelungsgrössen

$$\pi_{i1}, \ \pi_{i2}, \cdots \pi_{ie}$$

genügen einer in $K(\varepsilon)$ irreduziblen Gleichung e^{ten} Grades

$$\psi^{(i)}(\pi) = \pi^e + p\,C_{e-1}^{(i)}\,\pi^{e-1} + \cdots + p\,C_0^{(i)} = 0,$$

deren Koeffizienten $C_k^{(i)}$ ganze Grössen des Bereiches $K(1, \varepsilon)$ sind. Hierbei geht allgemein die Funktion

$$\psi^{(i)}(\pi) \quad \text{aus} \quad \psi^{(1)}(\pi)$$

dadurch hervor, dass man in den Koeffizienten $C_{e-1}^{(1)}, \cdots C_0^{(1)}$ die Grösse ε durch die konjugierte ε^{p^i} ersetzt.

§ 5. Allgemeine Bemerkung über die Behandlung der Zerlegungsgruppe.

Bevor auf die Beziehung der Wurzelentwicklungen zu den Gruppeneigenschaften von Z eingegangen wird, soll folgendes über die Behandlung der Zerlegungsgruppe Z bemerkt werden.

Seien

$$\alpha,\ \Theta_{12}(\alpha),\ \Theta_{13}(\alpha),\ \cdots\ \Theta_{fe}(\alpha) \qquad (1)$$

die Wurzeln von f(x) und

$$\xi = \xi(\alpha)$$

eine für den Bereich von p primitive Grösse des Körpers $K(p,\alpha)$, d. h. ein Ausdruck von der Form

$$\xi(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1},$$

wo $a_0, a_1, \cdots a_{n-1}$ Grössen aus K(p) sind, welcher einer in K(p) irreduktiblen Gleichung n^{ten} Grades genügt. Die sämtlichen Konjugierten von ξ sind dann

$$\xi(\alpha),\ \xi[\Theta_{12}(\alpha)],\ \cdots\ \xi[\Theta_{fe}(\alpha)]. \qquad (2)$$

Dann kann man auf dieselbe Weise, wie es in der Algebra für algebraische Grössen aus $K(1,\alpha)$ geschieht, folgende Sätze beweisen:

Die Grösse α lässt sich rational durch ξ ausdrücken in der Form

$$\alpha = b_0 + b_1\xi + \cdots + b_{n-1}\xi^{n-1},$$

wo die Koeffizienten $b_0, \cdots b_{n-1}$ dem Bereiche K(p) angehören.

Die Konjugierten von ξ lassen sich ebenfalls durch ξ rational ausdrücken mit Koeffizienten aus K(p), so dass wir sie folgendermassen schreiben können:

$$\xi,\ \varphi_{12}(\xi),\ \varphi_{13}(\xi),\ \cdots\ \varphi_{fe}(\xi). \qquad (3)$$

Die Reihenfolge der Konjugierten sei dieselbe wie in (2).

Die Gruppe, welche durch die Substitutionen (3) gebildet wird, ist isomorph mit der Gruppe der Substitutionen (1), und zwar derart, dass allgemein $\Theta_{ik}(\alpha)$ zugeordnet ist der Substitution $\varphi_{ik}(\xi)$.

Wir sind daher, um die Eigenschaften der Zerlegungsgruppe Z zu studieren, berechtigt, irgend eine primitive Grösse des Körpers $K(p,\alpha)$ zu wählen. Es ist am zweckmässigsten, die Entwicklungsgrösse π selbst zu wählen, die wir nach A § 15 als primitiv voraussetzen können. Nach

dem Schema des § 3 entsprechen den konjugierten Wurzeln von f(x)

$$\alpha_{11}, \alpha_{12}, \cdots \alpha_{fe}$$

der Reihe nach die konjugierten Entwicklungsgrössen

$$\pi_{11}, \pi_{12}, \cdots \pi_{fe}.$$

§ 6. Die Koeffizientengruppe T und der Koeffizientenkörper K(ε).

Die in K(p) irreduktible Funktion

$$(x-\pi_{11})(x-\pi_{12})\cdots(x-\pi_{fe})$$

zerfällt durch Adjunktion von ε in die bereits erwähnten f Faktoren vom e^{ten} Grade:

$$\psi^{(i)}(x) = (x-\pi_{i1})(x-\pi_{i2})\cdots(x-\pi_{ie}) = x^e + p\,C_{e-1}^{(i)}x^{e-1} + \cdots + pC_0^{(i)},$$

welche dadurch aus einander hervorgehen, dass man in den Koeffizienten die Grösse ε der Reihe nach durch $\varepsilon^p, \varepsilon^{p^2}, \cdots \varepsilon^{p^{f-1}}$ ersetzt.

Wegen der Irreduktibilität der Gleichung in K(ε) gehören die konjugierten Wurzeln der Gleichung $\psi^{(1)}(x) = 0$:

$$\pi_{11}, \pi_{12}, \cdots \pi_{1e}$$

zu einer Untergruppe e^{ten} Grades der Zerlegungsgruppe Z, welche „Koeffizientengruppe“ genannt und zur Abkürzung mit T bezeichnet werden soll. Der Beweis dafür wird ebenso geführt wie in § 1 für die Wurzeln von $f_1(x)$. Nur haben wir es hier mit dem Körper K(p,ε), nicht mit K(p), zu tun, was nach der Bemerkung in A § 15 an dem Beweisgange nichts ändert.

Wie man aus dem Schema des § 4 erkennt, „gehört“ die Grösse ε zu der Gruppe T, d. h. sie ändert sich nicht, wenn man auf sie eine Substitution von T anwendet, und ändert sich, wenn man auf ε eine andere Substitution der Gruppe Z anwendet. (cfr. Weber, Algebra Bd. I, 2. Aufl. § 161).

Sei

$$T,\ Tz,\ Tz^{(2)}, \cdots Tz^{(f-1)} \qquad (1)$$

das System der Nebengruppen von T, so gehören die zu ε konjugierten Grössen

$$\varepsilon,\ \varepsilon^{p},\ \varepsilon^{p^2}, \cdots \varepsilon^{p^{f-1}}$$

zu den konjugierten Gruppen

$$T,\ z^{-1}Tz,\ z^{(2)^{-1}}Tz^{(2)}, \cdots z^{(f-1)^{-1}}Tz^{(f-1)}. \qquad (2)$$

Es möge ε^{p^i} zu der Gruppe $z^{(i)^{-1}}Tz^{(i)}$ gehören, so folgt, da ε^{p^i} durch die Substitutionen von T nicht geändert wird, dass die Gruppe T mit der Gruppe $z^{(i)^{-1}}Tz^{(i)}$ identisch ist. Die Gruppen (2) sind also mit einander identisch, d. h. T ist ein Normalteiler der Gruppe Z. Die Reihe (1) kann man dann auch in der Form

$$T,\ zT,\ z^{(2)}T, \cdots z^{(f-1)}T \qquad (3)$$

schreiben.

Wenn z eine Substitution ist, welche ε in ε^p überführt, so geht ε durch die Anwendung der Substitutionen $z^2, \cdots z^{f-1}$ der Reihe nach in $\varepsilon^{p^2}, \cdots \varepsilon^{p^{f-1}}$ über. Die Nebengruppe z^iT enthält dann alle und nur die Substitutionen aus Z, die ε in ε^{p^i} überführen; und so sind die Nebengruppen (1) der Reihe nach mit den Nebengruppen

$$T,\ zT,\ z^2T, \cdots z^{f-1}T$$

identisch.

Da die Substitutionen t der Koeffizientengruppe T den Koeffizientenkörper ungeändert lassen, so geht durch eine solche jede Grösse aus $K(\alpha)$:

$$\xi = \varepsilon_0 + \varepsilon_1 \pi_{ik} + \varepsilon_2 \pi_{ik}^2 + \cdots$$

in eine andere von der Form

$$t(\xi) = \varepsilon_0 + \varepsilon_1 \pi_{ik'} + \varepsilon_2 \pi_{ik'}^2 + \cdots$$

über, in der die Koeffizienten ungeändert geblieben sind. Die Substitutionen t der Koeffizientengruppe sind also da-

durch ausgezeichnet, dass für jede Grösse ξ des Körpers die Kongruenz

$$t(\xi) \equiv \xi \qquad (\text{mod } \pi)$$

besteht.

Den nicht in T enthaltenen Substitutionen kommt diese Eigenschaft nicht zu. Denn eine solche Substitution, die man allgemein in der Form $z^i t$ $(i = 1,2 \cdots f-1)$ schreiben kann, führt die Grösse ε in ε^{p^i} über, welche beiden Grössen einander nicht modulo π kongruent sein können. ε und ε^{p^i} genügen ja beide der modulo p irreduziblen (vgl. A § 11) Kongruenz

$$\varphi(x) = x^f + c_1 x^{f-1} + \cdots + c_{f-1} \equiv 0 \qquad (\text{mod } \pi).$$

Diese würde, wie man mit Hilfe des Euklidschen Algorithmus leicht zeigen kann, modulo p zerfallen, wenn sie zwei modulo π kongruente Wurzeln hätte.

Im Koeffizientenkörper $K(\varepsilon)$ ist p immer noch Primfaktor. In ihm tritt also noch keine weitere Zerlegung des Primideals $\mathfrak{p}$ ein. Nur wird der Grad des letzteren von 1 auf f erhöht. Die Anzahl aller modulo p inkongruenten Grössen aus $K(\varepsilon)$ ist ja gleich p^f.

§ 7. Bau der Koeffizientengruppe T und des Körpers $K(\pi,\varepsilon)$ für den Fall, dass e durch p nicht teilbar ist.

Bei der weiteren Untersuchung der Galoisschen Gruppe wollen wir zunächst den einfacheren Fall betrachten, dass e durch p nicht teilbar ist. Es ist bereits im allgemeinen Teile bemerkt worden, dass dann in $K(p,\alpha)$ eine Grösse π existiert, welche der Gleichung

$$\pi^e + pC_0 = 0 \qquad (1)$$

genügt, wo C_0 eine modulo p reduzierte Einheit aus $K(\varepsilon)$ ist.

Diese Gleichung ist bekanntlich zyklisch im Rationalitätsbereiche der e^{ten} Einheitswurzeln. Also bilden die in $K(p)$ rationalen Substitutionen, welche die konjugierten Wurzeln dieser Gleichung in einander überführen, d. s. die Sub-

stitutionen der Trägheitsgruppe T, eine zyklische Gruppe. Der Galoissche Körper ist demnach ein relativzyklischer in bezug auf den Koeffizientenkörper.

Die Wurzeln der Gleichung (1) sind

$$\pi,\ \pi\gamma,\ \pi\gamma^2,\ \cdots\ \pi\gamma^{e-1}, \qquad (2)$$

wo $\gamma = e^{\frac{2\pi i}{e}}$ eine primitive Wurzel der Gleichung

$$x^e - 1 = 0 \qquad (3)$$

bedeutet.

Wegen der Eigenschaft des Galoisschen Körpers ist $\pi\gamma$, also auch die algebraische Einheit γ selbst in $K(\pi)$ enthalten. Nun genügt jede Einheit aus $K(\pi)$ (vergl. A, § 10), also auch γ der Kongruenz

$$x^{p^f-1} \equiv 1 \qquad (\text{mod } \pi). \qquad (4)$$

Da die Diskriminante der Gleichung (3) nicht durch p teilbar ist, also sämtliche Wurzeln dieser Gleichung $\gamma,\ \gamma^2,\ \cdots\ \gamma^{e-1}$ modulo π inkongruent sein müssen, so kann die Kongruenz

$$\gamma^e \equiv 1 \qquad (\text{mod } \pi)$$

für keinen niedrigeren Exponenten als e bestehen.

Dies verträgt sich nur dann mit der Kongruenz (4), wenn e ein Teiler von p^f-1 ist. Denn wäre e nicht Teiler von p^f-1, so könnte man p^f-1 in der Form

$$p^f-1 = eq + r$$

schreiben, wo $r > 0$ und $< e$ wäre. Es beständen dann zu gleicher Zeit die Kongruenzen

$$\left.\begin{array}{ll}\gamma^{eq+r} \equiv 1 & (5)\\ \gamma^e \equiv 1. & (6)\end{array}\right\} \ (\text{mod } \pi)$$

Erhebt man die zweite dieser Kongruenzen auf die 9te Potenz und multipliziert sie dann mit γ^r, so erhält man die Kongruenz

$$\gamma^{eq+r} \equiv \gamma^r \qquad (\text{mod } \pi),$$

und aus dieser unter Benützung von (5):

$$\gamma^r \equiv 1 \qquad (\mathrm{mod}\ \pi).$$

Eine solche Kongruenz darf aber nicht bestehen; denn es war oben bewiesen worden, dass die Kongruenz

$$\gamma^x \equiv 1 \qquad (\mathrm{mod}\ \pi)$$

für keinen niedrigeren Exponenten als $x = e$ bestehen kann. Und hierin liegt der Widerspruch. Wir können also setzen:

$$p^f - 1 = e \cdot a.$$

Da ε primitive Einheitswurzel von der Ordnung $p^f - 1$ war, so ist

$$\gamma = \varepsilon^a,$$

und die zu π konjugierten Grössen (2) sind gleich

$$\pi,\ \pi\varepsilon^a,\ \pi\varepsilon^{2a},\ \cdots\ \pi\varepsilon^{(e-1)a}.$$

Die Ableitung nach π

$$\psi'(\pi) = (\pi - \pi_1)(\pi - \pi_2) \cdot \cdot \cdot (\pi - \pi_{e-1})$$

ist also genau durch π^{e-1} teilbar, die vollständige Norm von $\psi'(\pi)$ also genau durch $p^{f(e-1)}$ teilbar. Da die $(\nu - 1)$ übrigen idealen Primfaktoren von p dieselbe Beschaffenheit wie $\mathfrak{p}$ besitzen, so ist nach A, § 14 die Diskriminante eines solchen Galoisschen Körpers genau durch $p^{f(e-1)\nu}$ teilbar.

§ 8. Die Zerlegung der Koeffizientengruppe für den Fall, dass e durch p teilbar. Die Verzweigungsgruppe 1. Ordnung $\overline{V}$ und der Körper $K(\overline{\pi}, \varepsilon)$.

Wurde in dem betrachteten Falle, wo e durch p nicht teilbar ist, der Zusammenhang zwischen der Gruppe und der Zerlegung des Primideals bereits festgestellt durch die Einführung des Koeffizientenkörpers, so genügt diese Einführung noch nicht im allgemeinen Falle, bei welchem e durch p teilbar ist. Da gelingt es nicht, eine Entwickelungsgrösse $\pi \backsim p^{\frac{1}{e}}$ aus $K(p, \alpha)$ zu finden, welche einer ähnlich einfachen Gleichung in $K(\varepsilon)$ genügt, wie bei dem speziellen

Falle. Der Grund dafür liegt in dem Umstande, dass die Koeffizientengruppe T so kompliziert gebaut sein kann, dass die Gleichung für π erst durch wiederholte Adjunktion von Abelschen Körpern lösbar wird.

Sei nunmehr e durch p teilbar:

$$e = p^s \bar{e}.$$

Wir werden uns nun einen Unterkörper von $K(\pi,\varepsilon)$ konstruieren, der im Rationalitätsbereiche des Koeffizientenkörpers $K(\varepsilon)$ den Grad $\bar{e}$ besitzt, und in welchem die Primzahl p nur der $\bar{e}^{\text{ten}}$ Potenz eines Primfaktors äquivalent ist.

Die Entwickelungsgrösse π genüge der Gleichung in $K(\varepsilon)$:

$$\pi^e + p\,C_{e-1}\pi^{e-1} + \cdot\cdot\cdot + p\,C_1\pi + p\,C_0 = 0$$

Es sei dann

$$\bar{\pi} = \pi^{p^s}.$$

Dann genügt $\bar{\pi}$ der Kongruenz

$$\bar{\pi}^{\bar{e}} + p\,C_0 \equiv 0 \qquad (\text{mod } \pi^{p^s\bar{e}+1}) \qquad (1)$$

Nun kann man die Einheit λ aus $K(\varepsilon)$ und die ganze Zahl r so bestimmen, dass die zu $\bar{\pi}$ äquivalente Grösse

$$\bar{\pi}(1 + \lambda\pi^r) = \pi^{p^s}(1 + \lambda\pi^r)$$

die Kongruenz (1) mindestens für $\pi^{p^s\bar{e}+2}$ als Modul befriedigt. Es sei nämlich die linke Seite der Kongruenz (1)

$$\left(\pi^{p^s}\right)^{\bar{e}} + p\,C_0 = \pi^{p^s\bar{e}+1+\rho}\,c$$

und c eine Einheit aus $K(\pi,\varepsilon)$. Dann besteht die Gleichung

$$[\pi^{p^s}(1 + \lambda\pi^r)]^{\bar{e}} + p\,C_0 = \pi^{p^s\bar{e}+1+\rho} \cdot c + \pi^{p^s\bar{e}+r}\,(\bar{e}\lambda + \pi^r a),$$

wo a eine beliebige ganze Grösse aus $K(\pi,\varepsilon)$ ist Wir bestimmen r aus der Gleichung

$$1 + \rho = r$$

sowie λ aus der Kongruenz

$$c + \bar{e}\lambda \equiv 0 \qquad (\text{mod } \pi).$$

Dann besteht sicher die Kongruenz

$$[\pi^{p^s}(1+\lambda\pi^r)]^{\bar{e}} + p C_0 \equiv 0 \qquad (\text{mod } \pi^{p^s \bar{e}+p+2}).$$

So fortfahrend erkennt man, dass in $K(\pi,\varepsilon)$ eine Grösse $\bar{\pi}$ vorhanden ist, welche der Gleichung

$$\bar{\pi}^{\bar{e}} + p C_0 = 0 \qquad (2)$$

genügt. Der Körper $K(\bar{\pi},\varepsilon)$ ist der gesuchte Körper. In ihm ist p der $\bar{e}^{\text{ten}}$ Potenz des Primfaktors $\bar{\pi}$ äquivalent.

Die bezüglich $K(\varepsilon)$ Konjugierten von $\bar{\pi}$ sind

$$\bar{\pi},\ \bar{\pi}\bar{\gamma},\ \bar{\pi}\bar{\gamma}^2, \cdots \bar{\pi}\bar{\gamma}^{\bar{e}-1},$$

wo $\bar{\gamma}$ die primitive Wurzel der Gleichung

$$x^{\bar{e}} - 1 = 0$$

ist. Da die Konjugierten sämtlich dem Körper $K(\pi,\varepsilon)$ angehören, gehört auch die Einheitswurzel γ diesem Körper an. Es folgt wie in § 7, dass $\bar{e}$ ein Teiler von p^f-1 ist. Wir setzen

$$\bar{e} \cdot a = p^f - 1, \text{ also } \bar{\gamma} = \varepsilon^a.$$

Die Konjugierten von $\bar{\pi}$ sind modulo $\bar{\pi}^2$ unter einander inkongruent. Der Körper $K(\bar{\pi},\varepsilon)$ ist in bezug auf $K(\varepsilon)$ relativ zyklisch vom Grade $\bar{e}$.

Ersetzt man in der Gleichung

$$\pi^{p^s} = \bar{\pi}\cdot\sigma = \bar{\pi}\,(\varepsilon_0 + \varepsilon_1\pi + \cdots + \varepsilon_{e-1}\pi^{e-1})$$

die Potenzen π^{p^s}, π^{2p^s}, $\cdots$ der Reihe nach durch $\bar{\pi}\cdot\sigma$, $\bar{\pi}^2\cdot\sigma^2$, $\cdots$ und fasst dann die mit $1, \pi, \pi^2, \cdots \pi^{p^s-1}$ multiplizierten Glieder zusammen, so erkennt man, dass π einer Gleichung vom Grade p^s genügt von der Form

$$\pi^{p^s} + \bar{\pi}\,\bar{C}_{p^s-1}\pi^{p^s-1} + \cdots + \bar{\pi}\,\bar{C}_0 = 0, \qquad (3)$$

in welcher die Koeffizienten aus $K(\overline{\pi},\varepsilon)$ sind, und $\overline{C}_0$ eine Einheit ist. Aus der Irreduktibilität dieser Gleichung folgt, dass die p^s Wurzeln dieser Gleichung durch die Substitutionen einer Untergruppe der Trägheitsgruppe vom $p^{s\,\text{ten}}$ Grade aus einander hervorgehen. Diese Untergruppe soll die „Verzweigungsgruppe 1ter Ordnung" heissen und zur Abkürzung mit $\overline{V}$ bezeichnet werden. Den zu $\overline{V}$ gehörigen Körper $K(\overline{\pi},\varepsilon)$ nennen wir den „Verzweigungskörper 1ter Ordnung".

Da $K(\overline{\pi},\varepsilon)$ relativ zyklisch ist in bezug auf den Koeffizientenkörper $K(\varepsilon)$, so ist die Verzweigungsgruppe 1ter Ordnung ein Normalteiler der Koeffizientengruppe T und man kann eine solche nicht zu $\overline{V}$ gehörige Substitution t von T finden, dass sich sämtliche Nebengruppen von $\overline{V}$ bezüglich T in der Form

$$\overline{V},\ \overline{V}t,\ \overline{V}t^2,\ \cdots\ \overline{V}t^{e-1}$$

darstellen lassen.

Die p^s Wurzeln der Gleichung (3) sind alle einander modulo π^2 kongruent.

Es seien nämlich π und $\pi' = c_1\pi + c_2\pi^2 + \cdots$ zwei Wurzeln der Gleichung (3), so bestehen die beiden Kongruenzen

$$\left.\begin{aligned} \pi^{p^s} + \overline{\pi}\,\overline{C}_0 &\equiv 0 \\ (c_1\pi + c_2\pi^2 + \cdots)^{p^s} + \overline{\pi}\,\overline{C}_0 &\equiv 0, \end{aligned}\right\} \quad (\text{mod } \pi^{p^s+1}) \qquad (4)$$

für deren zweite man offenbar auch schreiben kann

$$c_1^{p^s}\pi^{p^s} + \overline{\pi}\,\overline{C}_0 \equiv 0 \qquad (\text{mod } \pi^{p^s+1}) \qquad (5)$$

Durch Subtraktion der beiden Kongruenzen (4) und (5) findet man

$$c_1^{p^s} \equiv 1 \qquad (\text{mod } \pi) \qquad (6)$$

Andrerseits genügt c_1 nach A, § 10 der Kongruenz

$$c_1^{p^f-1} \equiv 1 \qquad (\text{mod } \pi) \qquad (7)$$

Da p^s und p^f-1 teilerfremd sind, kann man zwei ganze, positive Zahlen x und y so bestimmen, dass die Gleichung

$$x(p^f-1) = 1 + yp^s \qquad (8)$$

besteht.

Durch Kombination der Gleichungen (6), (7) und (8) folgt dann die Kongruenz

$$c_1 \equiv c_1^{1+yp^s} \equiv c_1^{x(p^f-1)} \equiv 1.$$

Es besteht also in der Tat die Kongruenz

$$\pi^1 \equiv \pi \qquad (\text{mod } \pi^2).$$

Es ist aber nicht ausgeschlossen, dass diese Kongruenz auch für eine höhere Potenz von π als Modul gilt.

Allgemeiner besagt diese Tatsache, dass die Substitutionen der Verzweigungsgruppe $\overline{V}$ nur solche Grössen des Körpers in einander überführen, welche modulo π^2 kongruent sind. Für jede Grösse γ des Körpers $K(\pi,\varepsilon)$ besteht also die Kongruenz

$$\overline{\upsilon}(\gamma) \equiv \gamma \qquad (\text{mod } \pi^2),$$

wo $\overline{\upsilon}$ eine beliebige Substitution von $\overline{V}$ bedeutet.

Durch eine Substitution von V dagegen, die nicht zu $\overline{V}$ gehört und $\overline{\pi}$ etwa in $\varepsilon^a \overline{\pi}$ verwandelt, geht π in eine konjugierte Entwickelungsgrösse π' über, welche zu π nicht modulo π^2 kongruent ist. Denn da π der Gleichung (3) genügt, so befriedigt es auch die Kongruenz

$$\pi^{p^s} + \overline{\pi}\,\overline{C}_0 \equiv 0 \qquad (\text{mod } \pi^{p^s+1}).$$

Dann genügt π' der Kongruenz

$$\pi'^{p^s} + \varepsilon^a\,\overline{\pi}\,\overline{C}_0 \equiv 0 \qquad (\text{mod } \pi^{p^s+1}).$$

Wenn nun π und π' einander modulo π^2 kongruent wären, so bestände auch die Kongruenz

$$\pi^{p^s} \equiv \pi'^{p^s} \qquad (\text{mod } \pi^{p^s+1}).$$

Aus den drei letzten Kongruenzen würde dann die Bedingung

$$\varepsilon^a \equiv 1 \qquad (\text{mod } \pi),$$

folgen, worin der Widerspruch liegt.

§ 9. Die Verzweigungskörper höherer Ordnung[1]).

Die p^s aus π durch die Substitutionen der Verzweigungsgruppe $\bar{V}$ hervorgegangenen konjugierten Grössen waren alle einander modulo π^2 kongruent. Es sei nun l eine solche ganze Zahl, dass diese Grössen zu π modulo π^l sämtlich kongruent sind, während wenigstens eine von ihnen mod π^{l+1} nicht zu π kongruent ist.

Es gehören dann die Grössen, welche modulo π^{l+1} zu π kongruent sind, zu einer Untergruppe von $\bar{V}$, welche die „Verzweigungsgruppe 2ter Ordnung" genannt und zur Abkürzung mit $\bar{\bar{V}}$ bezeichnet werden soll.

Denn bestehen für zwei Substitutionen $\bar{\bar{\upsilon}}_i$ und $\bar{\bar{\upsilon}}_k$ von $\bar{\bar{V}}$ die Kongruenzen

$$\left.\begin{aligned} \bar{\bar{\upsilon}}_i(\pi) &\equiv \pi \\ \bar{\bar{\upsilon}}_k(\pi) &\equiv \pi, \end{aligned}\right. \qquad (\text{mod } \pi^{l+1})$$

so folgt durch deren Kombination die Kongruenz

$$\bar{\bar{\upsilon}}_i\, \bar{\bar{\upsilon}}_k(\pi) \equiv \bar{\bar{\upsilon}}_i(\pi) \equiv \pi \qquad (\text{mod } \pi^{l+1}).$$

Der Grad der Gruppe $\bar{\bar{V}}$ möge gleich $p^{\bar{s}}$ sein.

Sei ferner

$$\bar{\bar{V}},\ \bar{\upsilon}_1\bar{\bar{V}},\ \bar{\upsilon}_2\bar{\bar{V}},\ \cdots\ \bar{\upsilon}_{p^{s-\bar{s}}-1}\bar{\bar{V}} \qquad (1)$$

die Reihe der $p^{s-\bar{s}}$ Nebengruppen von $\bar{\bar{V}}$. Man sieht ohne weiteres, dass die durch die Substitutionen einer Nebengruppe aus π hervorgegangenen Konjugierten einander

[1]) vergl. D. Hilbert. Die Theorie der algebraischen Zahlkörper. § 44. Jahresbericht der deutschen Mathematiker-Vereinigung, Bd. IV.

auch modulo π^{l+1} kongruent sind. Die durch alle diese Nebengruppen aus π hervorgegangenen Grössen sind dann $p^{s-\bar{s}}$ Grössen von der Form

$$\pi,\ \pi + \varepsilon_1 \pi^l,\ \cdots \qquad \pi + \varepsilon_{p^{s-\bar{s}}-1}\, \pi^l \tag{2}$$

modulo π^{l+1} kongruent, so dass allgemein

$$\bar{\upsilon}_i \bar{\bar{V}} \equiv \pi + \varepsilon_i \pi^l \qquad (\text{mod } \pi^{l+1}).$$

Da die Koeffizienten in (2) von einander verschiedene Einheiten des Koeffizientenkörpers sind, so folgt, dass ihre Anzahl $p^{s-\bar{s}}-1$ nicht grösser als die Anzahl p^f-1 aller reduzierten Einheiten, also $s-\bar{s}$ nicht grösser als f sein darf.

Ferner sieht man ohne weiteres, dass den Grössen (2) in derselben Reihenfolge auch die Substitutionen der Nebengruppen

$$\bar{\bar{V}},\ \bar{\bar{V}}\bar{\upsilon}_1,\ \bar{\bar{V}}\bar{\upsilon}_2,\ \cdots\ \bar{\bar{V}}\bar{\upsilon}_{p^{s-\bar{s}}-1}$$

modulo π^{l+1} kongruent sind, so dass allgemein die Gleichung besteht:

$$\bar{\bar{V}}\bar{\upsilon}_i = \bar{\upsilon}_i \bar{\bar{V}},$$

welche besagt, dass $\bar{\bar{V}}$ invariante Untergruppe von $\bar{V}$ ist.

Ferner besteht auch die Gleichung

$$(\bar{\upsilon}_i \bar{\bar{V}})\ (\bar{\upsilon}_k \bar{\bar{V}}) = (\bar{\upsilon}_k \bar{\bar{V}})\ (\bar{\upsilon}_i \bar{\bar{V}}). \tag{3}$$

Denn es ist

$$\left.\begin{aligned} (\bar{\upsilon}_i \bar{\bar{V}})\ (\bar{\upsilon}_k \bar{\bar{V}}) &\equiv (\pi + \varepsilon_k \pi^l) + \varepsilon_i \pi^l \\ (\bar{\upsilon}_k \bar{\bar{V}})\ (\bar{\upsilon}_i \bar{\bar{V}}) &\equiv (\pi + \varepsilon_i \pi^l) + \varepsilon_k \pi^l. \end{aligned}\right\} \quad (\text{mod } \pi^{l+1})$$

Die auf den linken Seiten stehenden beiden Komplexe von Substitutionen sind also ein und derselben Grösse aus (2) kongruent. Sie sind demnach in der Tat gleich einer und derselben Nebengruppe aus der Reihe (1).

Die Gleichung (3) lehrt uns, dass der zur Gruppe $\bar{\bar{V}}$ gehörige Unterkörper von $K(\pi,\varepsilon)$ ein relativ Abelscher ist

in bezug auf $K(\bar\pi,\varepsilon)$. Sein Relativgrad in bezug auf diesen ist gleich $p^{s-\bar s}$. Die Entwickelungsgrösse $\bar\pi$ aus $K(\bar\pi,\varepsilon)$ ist also in ihm der $p^{s-\bar s}$ ten Potenz eines Primfaktors $\bar{\bar\pi}$ äquivalent:

$$\bar\pi \sim \bar{\bar\pi}^{s-\bar s}.$$

Der Galoissche Körper $K(\pi,\varepsilon)$ ist in bezug auf den Körper $K(\bar\pi,\varepsilon)$ vom Grade p^{s}, also die Grösse $\bar\pi$ äquivalent π^{s}.

Es sei nun $\upsilon_1(\pi)$ eine Substitution von einer der Nebengruppen zu $\bar{\bar V}$, etwa von $\bar\upsilon_1\,\bar{\bar V}$. Es besteht dann die Kongruenz

$$\bar\upsilon_1(\pi) \equiv \pi + \gamma_1\pi^l \qquad (\mathrm{mod}\ \pi^{l+1}),$$

wo γ_1 eine Einheit ist. Man erhält dann durch wiederholte Anwendung von $\bar\upsilon_1(\pi)$ die leicht zu beweisenden Kongruenzen

$$\left.\begin{aligned} \bar\upsilon_1^{\,2}(\pi) &\equiv \pi + 2\gamma_1\pi^l \\ \bar\upsilon_1^{\,3}(\pi) &\equiv \pi + 3\gamma_1\pi^l \\ &\vdots \\ \bar\upsilon_1^{\,p}(\pi) &\equiv \pi + p\gamma_1\pi^l. \end{aligned}\right\} \quad (\mathrm{mod}\ \pi^{l+1}) \qquad (4)$$

($\bar\upsilon_1^{\,2}(\pi)$ bedeutet hier symbolisch: $\bar\upsilon_1[\upsilon_1(\pi)]$, u. s. w.)

Die Substitution $\bar\upsilon_1^{\,p}(\pi)$ gehört also wieder der Verzweigungsgruppe 2ter Ordnung $\bar{\bar V}$ an. Die Relativgruppe des Körpers $K(\pi)$ in bezug auf $K(\bar\pi)$ enthält demnach ausser der Einheitssubstitution nur Substitutionen vom Grade p. Der Körper $K(\bar\pi)$ ist also nur dann relativ zyklisch in bezug auf $K(\bar\pi)$, wenn sein Relativgrad gleich p ist.

In derselben Weise wird nun die Verzweigungsgruppe 2ter Ordnung $\bar{\bar V}$ weiter behandelt. Es sei $\bar l > l$ eine solche ganze Zahl, dass alle ihre Elemente zu π modulo $\pi^{\bar l}$, aber nicht alle Elemente zu π auch modulo $\pi^{\bar l+1}$ kongruent sind. Dann wählt man die Elemente von $\bar{\bar V}$ aus, welche auch

modulo $\pi^{\bar{l}+1}$ zu π kongruent sind. Man zeigt dann ebenso wie vorher, dass diese Elemente eine neue Gruppe, die Verzweigungsgruppe dritter Ordnung $\overline{\overline{\overline{V}}}$ bilden. Ihre Anzahl ist also ein Teiler von $\bar{p}^{\bar{s}}$, z. B. gleich $p^{\bar{\bar{s}}}$. Die Verzweigungsgruppe dritter Ordnung $\overline{\overline{\overline{V}}}$ ist eine relativ Abelsche Gruppe in bezug auf $\overline{\overline{V}}$. Zu ihr gehört ein neuer Verzweigungskörper $K(\bar{\bar{\pi}})$, der in bezug auf $K(\bar{\pi})$ ein relativ Abelscher vom Relativgrade $p^{\bar{s}-\bar{\bar{s}}}$ ist. In diesem Körper ist $\bar{\bar{\pi}}$ der $p^{\bar{\bar{s}}}$ ten Potenz eines neuen Primfaktors $\bar{\bar{\bar{\pi}}}$ äquivalent. Die Elemente der Relativgruppe von $K(\bar{\bar{\bar{\pi}}})$ in bezug auf $K(\bar{\bar{\pi}})$ sind alle ausser dem Einheitselement vom Grade p. Die Substitutionen der Nebengruppen von $\overline{\overline{\overline{V}}}$:

$$\overline{\overline{\overline{V}}},\ \bar{\bar{\upsilon}}_1\overline{\overline{\overline{V}}},\ \cdots\ \bar{\bar{\upsilon}}_{p^{\bar{s}-\bar{\bar{s}}}-1}\overline{\overline{\overline{V}}}$$

sind modulo $\pi^{\bar{l}+1}$ den Grössen

$$\pi,\ \pi+\bar{\gamma}_1\pi^{\bar{l}},\ \cdots\ \pi+\bar{\gamma}_{p^{\bar{s}-\bar{\bar{s}}}-1}\pi^{\bar{l}}$$

kongruent, wo die Koeffizienten einander inkongruente Einheiten sind.

In derselben Weise geht die Verzweigung weiter, bis der letzte Verzweigungskörper gleich dem Körper $K(\pi)$ selbst ist.

Die Elemente der letzten Verzweigungsgruppe seien zu π modulo π^λ kongruent, wo λ grösser als l, $\bar{l}$, u. s. w. ist, und nicht alle Elemente zu π modulo $\pi^{\lambda+1}$ kongruent sind. Dann gibt es offenbar unter ihnen kein Element, welches letztere Eigenschaft besässe. Sei $\omega(\pi)$ eine der Substitutionen der letzten Verzweigungsgruppe, so ist $\omega^p(\pi)$, wie aus den Kongruenzen (4) hervorgeht, zu π auch mindestens modulo $\pi^{\lambda+1}$ kongruent. Dies ist nach dem

Gesagten nur dann möglich, wenn $\omega^p(\pi) = \pi$ ist. Die Elemente der letzten Verzweigungsgruppe haben also alle ausser dem Einheitselement den Grad p.

Sei ferner $\rho(\pi)$ ein Element der vorletzten Verzweigungsgruppe und nicht zugleich der letzten Verzweigungsgruppe angehörig, so gehört $\rho^p(\pi)$ der letzten Verzweigungsgruppe an. Ist $\rho^p(\pi)$ nicht gleich π, also der Grad von $\rho(\pi)$ grösser als p, so ist nach dem vorhergehenden Abschnitt sicher $\rho^{p^2}(\pi) = \pi$. Die Elemente der vorletzten Verzweigungsgruppe können also höchstens den Grad p^2 haben. So geht es fort. Sind also im Ganzen r Verzweigungsgruppen in einander geschachtelt, so kann kein Element der ersten Verzweigungsgruppe $\overline{V}$ von höherem als dem $p^{r\text{ten}}$ Grade sein.

Es sei $\varphi(\pi)$ ein beliebiges Element der Verzweigungsgruppe 2ter Ordnung $\overline{\overline{V}}$

$$\varphi(\pi) = \pi + \gamma_l\, \pi^l + \gamma_{l+1}\pi^{l+1} + \cdots,$$

wo γ_l von Null verschieden sein soll. Durch zweimalige Anwendung von $\varphi(\pi)$ erhält man die Substitution

$$\varphi^2(\pi) = (\pi + \gamma_l\pi^l + \cdots) + \gamma_l(\pi + \gamma_l\pi^l + \cdots)^l + \gamma_{l+1}(\pi + \gamma_l\pi^l + \cdots)^{l+1} + \cdots.$$

Hieraus folgt die Kongruenz

$$\varphi^2(\pi) \equiv 2\varphi(\pi) - \pi + l\gamma_l^2\pi^{2l-1} \qquad (\text{mod } \pi^{2l}).$$

Durch nochmalige Ausführung der Substitution $\varphi(\pi)$ erhält man die weiteren Kongruenzen:

$$\begin{aligned} \varphi^3(\pi) &\equiv 2\varphi^2(\pi) - \varphi(\pi) + l\gamma_l^2[\varphi(\pi)]^{2l-1} \\ &\equiv 4\varphi(\pi) - 2\pi + 2l\gamma_l^2\pi^{2l-1} - \varphi(\pi) + l\gamma_l^2\pi^{2l-1} \quad (\text{mod } \pi^{2l}) \\ &\equiv 3\varphi(\pi) - 2\pi + 3l\gamma_l^2\pi^{2l-1} \end{aligned}$$

Man erkennt bald, dass allgemein die Kongruenz

$$\varphi^{i}(\pi) \equiv i\varphi(\pi) - (i-1)\pi + \frac{i(i-1)}{2} l \gamma_l^{2} \pi^{2l-1} \qquad (\mathrm{mod}\ \pi^{2l})$$

besteht, die sich durch vollständige Induktion leicht verifizieren lässt.

Für $i = p$ erhält man dann die Kongruenz

$$\varphi^{p}(\pi) \equiv p\varphi(\pi) - (p-1)\pi + \frac{p(p-1)}{2} \gamma_l \pi^{2l-1} \qquad (\mathrm{mod}\ \pi^{2l})$$

oder unter Vernachlässigung des letzten Gliedes

$$\begin{aligned} \varphi^{p}(\pi) &\equiv p\varphi(\pi) - (p-1)\pi \\ &\equiv \pi + p\gamma_l \pi^{l} + p\gamma_{l+1} \pi^{l+1} + \cdots \qquad (\mathrm{mod}\ \pi^{2l}). \end{aligned}$$

Es sei $\omega(\pi)$ ein Element der letzten Verzweigungsgruppe:

$$\omega(\pi) = \pi + \gamma_\lambda \pi^{\lambda} + \gamma_{\lambda+1} \pi^{\lambda+1} + \cdots$$

Für dieses besteht dann auch die Kongruenz

$$\omega^{p}(\pi) \equiv \pi + p\gamma_\lambda \pi^{\lambda} + p\gamma_{\lambda+1} \pi^{\lambda+1} \qquad (\mathrm{mod}\ \pi^{2\lambda}).$$

Nun ist, wie vorhin bewiesen wurde, $\omega^{p}(\pi) = \pi$. Dies verträgt sich mit der letzten Kongruenz nur dann, wenn die Ordnung des Gliedes $p\gamma_\lambda \pi^{\lambda}$ nicht kleiner als 2λ ist, also wenn die Ungleichung besteht

$$2\lambda \leqq p^{s}\bar{e} + \lambda.$$

Es besteht also für λ die Ungleichung

$$\lambda \leqq p^{s}\bar{e}.$$

Der Exponent λ darf also nicht grösser sein, als die Ordnung von p in bezug auf π beträgt; die Exponenten $l, \bar{l}, \cdots$ müssen also kleiner sein als diese Ordnung.

§ 10. Die Diskriminante des Körpers $K(\pi)$.

Von der Art der Zerlegung der Koeffizientengruppe T und von den Exponenten $l, \bar{l}, \cdots$ hängt die Ordnung der Körperdiskriminante in bezug auf p ab.

Zur Ermittelung dieser Ordnung brauchen wir nur die Ordnung der Ableitung $\psi'(\pi)$ in bezug auf π zu bestimmen.

$$\psi'(\pi) = (\pi_1 - \pi)(\pi_2 - \pi) \cdots (\pi_{p^s \overline{e}-1} - \pi).$$

Von den Konjugierten $\pi_1, \pi_2 \cdots$ gehören $p^s(\overline{e}-1)$ zu den $\overline{e}-1$ Nebengruppen von V in bezug auf die Koeffizientengruppe T. Diese sind zu π modulo π^2 inkongruent. Jede der zugehörigen Differenzen in $\psi'(\pi)$ ist also genau durch π, ihr Produkt also genau durch $\pi^{p^s(\overline{e}-1)}$ teilbar.

Von den übrigen Konjugierten gehören $p^{\overline{s}}(p^{s-\overline{s}}-1) = p^s - p^{\overline{s}}$ zu den $p^{s-\overline{s}}-1$ Nebengruppen von $\overline{V}$ in bezug auf V. Sie sind zu π genau modulo π^l kongruent. Jede der zugehörigen Differenzen ist also genau durch π^l, ihr Produkt durch $\pi^{l(p^s - p^{\overline{s}})}$ genau teilbar.

So geht es weiter. Die Ordnung von $\psi'(\pi)$ ist demnach gleich

$$(p^s \overline{e} - p^s) + l(p^s - p^{\overline{s}}) + \overline{l}(p^{\overline{s}} - p^{\overline{\overline{s}}}) + \cdots.$$

Die Diskriminante des Körpers $K(\pi)$ ist dann nach A, § 14 genau teilbar durch:

$$p^{f\nu[(p^s \overline{e} - p^s) + l(p^s - p^{\overline{s}}) + \overline{l}(p^{\overline{s}} - p^{\overline{\overline{s}}}) + \cdots]}.$$

Lebenslauf.

Ich, Friedrich Hüttig, wurde geboren am 26. September 1881 zu Sagan in Schlesien, als Sohn des Pastors Bernhard Hüttig und seiner Frau Martha, geb. Schuricht. Ich besuchte von Ostern 1887 bis Ostern 1891 die Fürstentumsschule, bis Ostern 1900 das Kgl. Gymnasium zu Sagan. Während des Sommersemesters 1900 war ich an der Universität Marburg, während des Wintersemesters 1900/01 an der Universität Berlin immatrikuliert. Dann besuchte ich drei Semester lang die Breslauer Universität und war hierauf von Michaelis 1902 bis zum Februar des Jahres 1904 wieder an der Universität Marburg immatrikuliert. Zwei weitere Semester, grösstenteils in Marburg verlebt, dienten der Vorbereitung zur Prüfung für das höhere Lehramt, welche ich am 18. November 1904 bestand, und Vorarbeiten zu vorliegender Dissertation. Von Ostern 1905 bis Ostern 1906 verwaltete ich eine wissenschaftliche Hilfslehrerstelle an der Städt. Oberrealschule zu Oldenburg i. Gr., von Ostern 1906 bis jetzt eine solche an dem Kgl. König-Wilhelms-Gymnasium zu Breslau. Zugleich bin ich Mitglied des pädagogischen Seminars daselbst. Das Rigurosum bestand ich am 7. März des Jahres 1906.

Meine Studien galten der Mathematik, Physik, Biologie und Philosophie und verdanke ich auf diesen Gebieten reiche Anregung und Förderung meinen verehrten Lehrern, den Herren Dozenten: Cohen, Feussner, Hensel, Hess,
Jung, Kayser, Melde, A. Meyer, Natorp,
Richarz von der Marburger Universität,

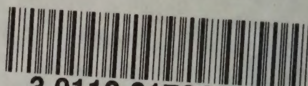
den Herren Dozenten: Brefeld, Ebbinghaus, Franz, Kükenthal, London, Neumann, Partsch, Rosanes, Sturm von der Breslauer Universität,

den Herren Dozenten: Diltey, Hettner, Knoblauch, F. E. Schulze, Wahnschaffe von der Berliner Universität.

Zu besonderem Danke bin ich Herrn Prof. Dr. Hensel verpflichtet, der mich in wichtige Gebiete der Mathematik, im besonderen in die algebraische Zahlentheorie, einführte und mir auch die Anregung zu vorliegender Arbeit gab.

Buchdruckerei H. Fleischmann, Breslau, Ohlauerstr. 8.

G.E. STECHERT
& Co.
NEW YORK


UNIVERSITY OF ILLINOIS-URBANA
512.32H97A C001
ARITHMETISCHE THEORIE EINES GALOISSCHEN
3 0112 017046183